

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

In re MAPFRE Data Disclosure Litigation * Civil Action No. 1:23-cv-12059-IT
*
*

MEMORANDUM & ORDER

March 31, 2025

TALWANI, D.J.

Before the court in this data-breach action is Defendants’ Motion to Dismiss [Doc. No. 48] Plaintiffs’ Consolidated Class Action Complaint [Doc. No. 45] for lack of standing and failure to state a claim for relief. For the reasons set forth below, the court denies the Motion as to Plaintiffs’ claims for violation of the Driver’s Privacy Protection Act (“DPPA”), 18 U.S.C. § 2724, and violation of Massachusetts General Laws, Chapter 93A (“Chapter 93A”), and grants the Motion as to Plaintiffs’ negligence, invasion-of-privacy, and declaratory judgment claims.

I. Background

A. The Data Disclosure

Lynne Alexandrowicz, Brian Conway, Fred Devereaux, Veronica Gregory, Richard Ma, Brian Ray, and Annemarie Whilton (collectively, “Massachusetts Plaintiffs”) as well as David Brule (with the Massachusetts Plaintiffs, “Plaintiffs”), allege the following facts, which the court assumes true for the purpose of deciding this motion:

Defendants MAPFRE U.S.A. Corp. and its subsidiary The Commerce Insurance Company (collectively “MAPFRE”) offer passenger automobile insurance to individuals throughout the United States. Am. Compl. ¶¶ 7, 31–32, 101 [Doc. No. 45]. MAPFRE implemented an online quoting platform (“Quote Platform”) on its website that allows prospective customers to obtain an instant insurance quote by providing basic personal

information. Id. at ¶¶ 7, 105, 190. To use the Quote Platform, a visitor to the website enters a name, date of birth, and address. Id. at ¶ 107. To encourage the website visitor to purchase an insurance policy, MAPFRE’s system then automatically populates a quote form with the driver’s license number associated with the personal information that the user provided. Id. at ¶¶ 9–10, 106–107.

A person’s name, date of birth, and address are often available to the public at no cost, and as a result are commonly obtained by cybercriminals. Id. at ¶ 107. Further, anyone can access the quote platform by visiting MAPFRE’s website, and the platform does not require verification that the visitor accessing the system and obtaining a quote is the individual whose information is entered into the Quote Platform. Id. at ¶¶ 105, 110.

In February 2021, the New York State Department of Financial Services (“DFS”) issued a public warning regarding an ongoing systemic and aggressive campaign by cybercriminals to engage with public-facing insurance websites that offer instant online automobile insurance quotes—like MAPFRE’s Quote Platform—to obtain unredacted driver’s license numbers. Id. at ¶ 121. The warning explained that “the unauthorized collection of driver’s license numbers appeared to be part of a growing fraud campaign targeting pandemic and unemployment benefits.” Id. In March 2021, DFS issued a second warning that urged companies like MAPFRE to stop employing quoting tools that displayed driver’s license numbers on their website in light of the “serious risk of theft and consumer harm.” Id. at ¶ 124.

MAPFRE nonetheless maintained the feature on its Quote Platform, see id. at ¶¶ 15, 119, and did not employ security or verification measures to prevent website visitors or a “bot” or automated process from entering other individuals’ information on the Quote Platform and thereby obtaining the individuals’ driver’s license numbers. See id. at ¶¶ 110, 128. MAPFRE’s

continued use of the Quote Platform without adequate security measures allowed scammers to use an automated process to harvest Plaintiffs’ and putative class members’ driver’s license numbers from the Quote Platform. Id. at ¶ 108.

Cybercriminals obtained driver’s license numbers for 266,142 individuals, id. at ¶¶ 14–15, by “specifically targeting” MAPFRE’s Quote Platform (“the Data Disclosure”), id. at ¶ 42. In a notice that MAPFRE sent on or about August 22, 2023, to individuals impacted by the Data Disclosure, MAPFRE confirmed that “[b]etween July 1 and July 2, 2023, an unknown party used information” about the individuals “to obtain access to additional information . . . through MAPFRE’s Massachusetts online quoting platform in Massachusetts,” including their driver’s license numbers and vehicle information (the “personal information” or “PI”). Id. at ¶¶ 15–16; see also id. at ¶ 118. According to the notice, MAPFRE took down the Quote Platform and implemented new protections against future incidents as soon as it became aware of the issue. Id. at ¶ 119.

MAPFRE’s notice also encouraged those affected by the Data Disclosure to “remain vigilant against incidents of identity theft and fraud, and to monitor [their] free credit reports for suspicious activity and . . . errors.” Id. at ¶ 130.

B. Alleged Potential Uses of Driver’s License Information

Driver’s license numbers can be used to file fraudulent unemployment claims. Id. at ¶¶ 94, 132, 134, 142. Further, driver’s license numbers can be used to commit other financial fraud, including opening bank accounts, applying for credit cards, and taking out loans. Id. at ¶¶ 132–33. An individual’s driver’s license number can be used to create fake driver’s licenses or to impersonate the victim during a job application process, while receiving medical treatment, and in interactions with law enforcement. Id. at ¶ 134. Finally, third parties can also use an

individual's driver's license number to obtain additional personal information that can be used to commit identity fraud. Id. Someone in possession of an individual's driver's license number can "socially engineer" that individual into providing additional personal information. See id. at ¶ 134–35. Further, individuals can sell a driver's license number to another who possesses a victim's other personal information to create a complete identity profile. Id. at ¶ 135–36. Unique and persistent identifiers such as driver's license numbers are critical to forging an identity. Id. at ¶ 135.

C. Plaintiffs' Injuries

Each Plaintiff has "spent considerable time and effort" responding to the Data Disclosure and continues to take "considerable precautions, to monitor for and protect against the unauthorized dissemination of [his or her] driver's license number and PI." Id. at ¶ 40; see also id. at ¶¶ 46, 54, 62, 67, 76, 84, 97 (same). After receiving notice of the disclosure, each Plaintiff spent several hours researching the breach, contacting MAPFRE, and monitoring accounts. Id. at ¶¶ 38, 40, 44, 46, 51, 54, 60, 62, 66, 67, 73, 76, 82, 84, 88, 97. Plaintiffs dealt further with any fallout of the Data Disclosure as follows:

Plaintiff Annemarie Whilton discovered shortly after the July 1 Data Disclosure that she was a victim of unemployment benefits fraud. Id. at ¶ 90. On or about July 5, 2023, Whilton attempted to apply for Massachusetts unemployment benefits online. Id. at ¶ 91. However, the Massachusetts agency's website informed her that she could not submit the application because a claim had already been submitted in her name. Id. Whilton subsequently drove to the Unemployment Office in Quincy, Massachusetts, to apply for benefits in person. Id. at ¶ 92. She waited several hours before speaking with an employee who told her to go to the Social Security Administration Office in Quincy. Id. An employee in that office told her to contact Boston Police

and visit the Boston Office for Unemployment Assistance. Id. At the Boston unemployment office, Whilton submitted a Fraud Reporting Form. Id. at ¶ 93. The Commonwealth of Massachusetts Department of Unemployment Assistance emailed her on or about July 6, 2023, informing her that if a fraudulent claim was filed in her name, she was “likely the victim of an earlier national or private sector data breach,” and that “[i]t is likely that . . . criminal enterprises were in possession of your [PI] in order to file a fraudulent claim.” Id.

After receiving this information, Whilton requested to update her Multi-Factor Authentication information with the Unemployment Assistance Department. Id. at ¶ 94. To submit this request, Whilton submitted a form that required her to provide her Massachusetts driver’s license number. Id. Whilton did not receive unemployment benefits until approximately seven weeks after her initial application. Id. at ¶ 95.

Whilton, Brian Conway, and Richard Ma discovered fraudulent charges to their debit or credit cards in the months after the incident. Id. at ¶¶ 53 (Conway), 75 (Ma), 96 (Whilton). Additionally, Brian Ray became aware that several lines of credit had been opened in his name when he contacted credit bureaus after learning of the Data Disclosure. Id. at ¶ 83.

D. Plaintiffs’ Claims

Plaintiffs’ Consolidated Class Action Complaint (the “Amended Complaint”) [Doc. No. 45] asserts five causes of action stemming from the data disclosure: a violation of the Driver’s Privacy Protection Act, 18 U.S.C. §§ 2724, et seq., Am. Compl. ¶¶ 180–96, negligence, id. at ¶¶ 197–216, violation of Massachusetts General Laws, Chapter 93A, id. at ¶¶ 217–31, invasion of privacy, id. at ¶¶ 232–38, and a claim for declaratory and injunctive relief, id. at ¶¶ 239–47. All causes of action except the Chapter 93A claim are asserted by Plaintiffs on behalf of a putative nationwide class, or in the alternative, by the Massachusetts Plaintiffs on behalf of a

putative Massachusetts class; the Chapter 93A claim is brought only by the Massachusetts Plaintiffs on behalf of a putative Massachusetts class. See id. at ¶¶ 217–31.

Plaintiffs allege the disclosure of their driver’s license numbers to third parties harmed them in several ways, including:

invasion of privacy; loss of privacy; loss of control over PI and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PI; harm resulting from damaged credit scores and credit information; a substantially increased risk of future identity theft and fraud; loss of time and money preparing for and resolving fraud and identity theft; [and] loss of time and money obtaining protections against future identity theft[.]

Id. at ¶ 170.

Each Plaintiff seeks actual and statutory damages, and injunctive relief, “including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of [his or her] PI that Defendants disclosed in the Data Disclosure,” and enjoining Defendants from continuing the alleged unlawful practices. Id. at ¶ 43; see also id. at ¶¶ 49, 57, 65, 70, 79, 87, 100 (same); id. at p. 69 (Prayer for Relief).

MAPFRE has filed a Motion to Dismiss the Consolidated Class Action Complaint (“Motion to Dismiss”) [Doc. No. 48], which Plaintiffs have opposed. Opp’n [Doc. No. 53].

II. Discussion

A. Standing

MAPFRE argues that Plaintiffs fail to plausibly allege standing. It asserts that the forms of financial fraud that the Plaintiffs allege cannot be committed with a driver’s license number, and that without plausible allegations of actual misuse, the allegations that Plaintiffs face a risk of future harm is insufficient to confer standing. Mem. ISO Mot. to Dismiss 6–12 [Doc. No. 49].

As explained below, the court finds Plaintiffs have alleged standing to pursue damages where they have alleged a plausible connection between the financial fraud they have suffered

and the Data Disclosure, and where they have alleged costs incurred in response to an imminent and substantial risk of future identity fraud. However, Plaintiffs have not plausibly alleged that the threat of future harm is redressable by the prospective relief that they seek. Consequently, they lack standing to pursue the injunctive and declaratory relief identified in the Amended Complaint.

1. Standard of Review

The doctrine of standing is rooted in Article III of the Constitution, which confines federal courts to the adjudication of actual “cases” and “controversies.” See U.S. Const. art. III, § 2, cl. 1; Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992). Standing consists of three elements: “[t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016) (citing Lujan, 504 U.S. at 560–61). Where no class is yet certified, the court “evaluate[s] only whether the [named] plaintiff[s] have] constitutional [] standing to pursue the action.” Katz v. Pershing, LLC, 672 F.3d 64, 71 (1st Cir. 2012). Plaintiffs bear the burden to demonstrate that they have standing. TransUnion LLC v. Ramirez, 594 U.S. 413, 430–31 (2021). Further, “plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek” Id. at 431.¹

¹ At the motion hearing, Defendant argued that Plaintiffs’ standing to pursue each claim rises and falls together, and Plaintiff argued that the alleged DPPA violation provided an alternative path to standing as to that claim. Because Plaintiffs’ claims are intertwined and all alleged injuries arise from the Data Disclosure, the court analyzes standing as to all causes of action together. See Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 373 n.3 (1st Cir. 2023) (treating claims together in standing analysis because “[t]he claims asserted in the plaintiffs’ complaint all arise from the . . . data breach” and because neither party argued that the standing inquiry differs with respect to any claim”) (citing TransUnion, 594 U.S. at 439–42; In re Evenflo Co., Inc., Mktg., Sales Pracs. & Prod. Liab. Litig., 54 F.4th 28, 35 (1st Cir. 2022); Clemens v. ExecuPharm

To establish the first element of standing, an injury in fact, plaintiffs must demonstrate “an invasion of a legally protected interest” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.” Spokeo, 578 U.S. at 339 (quoting Lujan, 504 U.S. at 560). “The most obvious” concrete harms “are traditional tangible harms, such as physical harms and monetary harms.” TransUnion, 594 U.S. at 425. “Intangible harms can also be concrete, including when they ‘are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts’ such as ‘reputational harms, disclosure of private information, and intrusion upon seclusion.’” Webb, 72 F.4th at 372 (quoting TransUnion, 594 U.S. at 425). “[A] material risk of future harm can [also] satisfy the concrete-harm requirement,’ at least as to injunctive relief, when ‘the risk of harm is sufficiently imminent and substantial.’” Id. at 375 (quoting TransUnion, 594 U.S. at 435) (alterations in original). However, “to have standing to pursue damages based on a risk of future harm, plaintiffs must demonstrate a separate concrete harm caused ‘by their exposure to the risk itself.’” Id. at 372 (quoting TransUnion, 594 U.S. at 437) (emphasis omitted).

The second element, traceability, “requires the plaintiff[s] to show a sufficiently direct causal connection between the challenged action and the identified harm.” In re Evenflo Co., 54 F.4th at 34 (quoting Katz, 672 F.3d at 71). And to show redressability, the third element, the plaintiff must demonstrate that favorable resolution by the court would remedy the alleged injury. Id.

Because standing is not a “mere pleading requirement[] but rather an indispensable part of the plaintiff’s case,” standing must be supported “with the manner and degree of evidence

Inc., 48 F.4th 146, 156-59 (3d Cir. 2022)). Finding standing as to all claims seeking monetary relief, the court does not address Plaintiffs’ alternative argument as to the DPPA claim.

required at the successive stages of the litigation.” Lujan, 504 U.S. at 561; see also TransUnion LLC, 594 U.S. at 431. At the pleading stage, “the plaintiff must ‘clearly . . . allege facts demonstrating’ each element” of standing. Spokeo, 578 U.S. at 338 (quoting Warth v. Seldin, 422 U.S. 490, 518 (1975)) (alterations in original). The court applies “the same plausibility standard used to evaluate a motion under Rule 12(b)(6)” in determining whether Plaintiffs have alleged standing. Webb, 72 F.4th at 371 (quoting Gustavsen v. Alcon Lab’ys, Inc., 903 F.3d 1, 7 (1st Cir. 2018)).

2. Injury in Fact

Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365 (1st Cir. 2023), controls whether Plaintiffs have adequately alleged an injury in fact. In Webb, two patients brought a putative class action arising from a data breach in which hackers infiltrated a pharmacy’s patient records system and obtained patient PI, including names and social security numbers. Id. at 370. One patient alleged that her information was used to file a fraudulent tax return and that she “expended considerable time” communicating with the IRS to resolve issues associated with the fraudulent return. Id. Additionally, both plaintiffs alleged that they spent “considerable time and effort monitoring [their] accounts to protect [themselves] from . . . identity theft.” Id. at 376.

The First Circuit first held that the complaint sufficiently alleged a concrete injury in fact as to the first plaintiff—actual misuse of her PI—because it included plausible allegations that third parties had obtained her data and used it to file a fraudulent 2021 tax return. Id. at 370, 373. Because the data breach had occurred in January 2021, the complaint alleged “an obvious temporal connection” between the data breach and the filing of the fraudulent tax return. Id. at 374. Additionally, the complaint alleged that the first plaintiff was “very careful about sharing her [PI], has never knowingly transmitted unencrypted [PI] over the internet or any other

unsecured source, and stores documents containing her [PI] in a secure location.” Id. (internal quotations omitted). “The obvious inference” to draw from these allegations was that the perpetrator of the fraudulent tax return obtained her information in the data breach. Id.

Next, although the complaint in Webb did not allege actual misuse of the second plaintiff’s PI, it included allegations that both plaintiffs took efforts to mitigate the risk of future misuse of their PI, and those efforts constituted a separate, concrete harm. Id. at 374–75. The First Circuit explained that allegations that data was obtained in a “targeted attack,” that some portion of the stolen data had already been misused, and that the compromised data is “particularly sensitive” all supported a conclusion that the stolen data is likely to be misused in the future. See id. at 375–76. The court determined that the risk of future misuse was “imminent and substantial” because the data breach was a targeted attack by cybercriminals who hacked into the pharmacy’s records to steal patient information. Id. at 376. Further, the complaint alleged that the first plaintiff’s data obtained in the attack had already been misused, and that the patient names and social security numbers that the hackers stole were sensitive data. Id. Therefore, the time and effort that both plaintiffs spent mitigating the risk of future identity theft constituted a concrete injury in response to a substantial and imminent risk rather than an attempt to “manufacture standing by incurring costs in anticipation of a non-imminent harm.” Id. at 377 (quoting Clapper v. Amnesty Int’l USA, 568 U.S. 398, 422 (2013)).

Here, as detailed below, the Amended Complaint likewise includes plausible allegations that some data exposed in the Data Disclosure has been misused. Based on those allegations and others demonstrating that the Data Disclosure was the result of a targeted attack to obtain Plaintiffs’ sensitive PI, all Plaintiffs face an imminent and substantial risk of future identity fraud such that their mitigation efforts constitute concrete injuries.

a. Actual Misuse

Under Webb, “actual misuse of [PI] may constitute an injury in fact.” 72 F.4th at 373. Here, several Plaintiffs have alleged instances of actual misuse of their driver’s license numbers that constitute concrete injuries.

Whilton has alleged that unauthorized third parties obtained her driver’s license number in the Data Disclosure, and that her PI was used to submit a fraudulent claim for unemployment benefits in her name shortly thereafter. See Am. Compl. ¶¶ 89–91. As in Webb, there is “an obvious temporal connection” between the Data Disclosure and the filing of the fraudulent claim. Webb, 72 F.4th at 374. MAPFRE’s notice informed Whilton that third parties obtained her driver’s license number between July 1 and July 2, 2023. Am. Compl. ¶ 89 [Doc. No. 45]. Plaintiffs allege that Whilton submitted an application for unemployment benefits on July 5, 2023, which was rejected because someone had already submitted an unemployment benefits claim using her personal information. Id. at ¶ 91. Further, the Amended Complaint alleges a plausible connection between the Data Disclosure and the fraudulent unemployment claim in Whilton’s name. Id. at ¶ 94. The Amended Complaint alleges that a driver’s license number can be used—and in Massachusetts is required—to apply for unemployment benefits and/or for the administration of those benefits. Id. at ¶¶ 94, 132, 142. It is reasonable to infer from these allegations that third parties obtained Whilton’s driver’s license number in the Data Disclosure and subsequently used it in filing a fraudulent claim for unemployment benefits.

In addition, Plaintiffs allege that Whilton, Conway, and Ma experienced fraudulent charges on their debit and credit cards in the months following the Data Disclosure. Id. at ¶¶ 53, 75, 96. Plaintiffs also allege that Ray “has experienced the fraudulent opening of several lines of credit in his name” since learning of the incident. Id. at ¶ 83. Where the Data Disclosure occurred

in July 2023, and Conway and Whilton incurred those charges in September and October respectively, id. at ¶ 53 (Conway); id. at ¶ 96 (Whilton), there is a temporal connection from these alleged charges to the Data Disclosure. There is a similar connection to Ma’s charges, which occurred in December 2023. Id. at ¶ 75. And although the Amended Complaint does not allege how long after the Data Disclosure that lines of credit were opened in Ray’s name, he alleged this harm in his first Complaint, which he filed on September 27, 2023. See id. at ¶ 83; see also Compl. ¶ 24, Ray v. MAPFRE U.S.A. Corp., No. 23-cv-12214, [Doc. No. 1]. Further, Plaintiffs allege that Whilton, Conway, Ma, and Ray were all “very careful about sharing . . . PI” and “never knowingly transmitted unencrypted PI over the internet or any other unsecured source.” Am. Compl. ¶¶ 55, 77, 85, 98 [Doc. No. 45]. Allegations that these Plaintiffs suffered from identity and financial fraud following the Data Disclosure combined with allegations that these Plaintiffs have not otherwise knowingly transmitted their unsecured PI support an inference that the actors responsible for these instances of fraud obtained Plaintiffs’ PI as a result of the data breach. See Webb, 72 F.4th at 374.

b. Cost to Mitigate Risk of Future Harm

Plaintiffs allege that they suffered an injury in the form of time spent mitigating the risk of future identity theft “that would have otherwise been put to other productive use.” Id. at ¶¶ 42, 48, 56, 64, 69, 78, 86, 99. The Amended Complaint includes allegations that Plaintiffs spent time contacting MAPFRE, monitoring accounts, freezing credit, and updating account security measures in response to the Data Disclosure. Id. at ¶¶ 46, 67, 76, 84, 94.

Time spent mitigating the risk of future harm created by a data breach can constitute “a separate concrete, present harm” that gives a plaintiff standing to pursue damages when that time would have otherwise been put to profitable use. Webb, 72 F.4th at 376. However, plaintiffs

“cannot manufacture standing by incurring costs in anticipation of non-imminent harm.”

Clapper, 568 U.S. at 422. Therefore, mitigations efforts must have been taken in response to “a substantial and imminent risk of harm” to constitute an injury in fact for standing purposes.

Webb, 72 F.4th at 377. In determining whether a risk of future misuse of personal information exposed in a data breach is imminent and substantial, the First Circuit has endorsed the following factors:

(1) whether the plaintiffs’ data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

Webb, 72 F.4th at 375 (quoting McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 302 (2d Cir. 2021)).

Here, Plaintiffs have sufficiently alleged facts supporting all three factors. First, the Amended Complaint alleges that each Plaintiff received notice that MAPFRE “determined that [an] unknown party obtained access to [their] driver’s license number[s] through MAPFRE’s Massachusetts online quoting platform” by inputting personal information obtained from other sources, and that “the Data Disclosure involved unauthorized third parties specifically targeting” MAPFRE’s Quote Platform. Am. Compl. ¶¶ 15–16, 42 [Doc. No. 45]. Second, the Amended Complaint alleges that several Plaintiffs’ PI has already been used to commit the sorts of fraud that the Amended Complaint alleges can be committed with a driver’s license number (in combination with other information).

Third, the Amended Complaint contains plausible allegations that a driver’s license number is sensitive “such that there is a high risk of identity theft or fraud” if it is exposed. Webb, 72 F.4th at 375 (quoting McMorris, 995 F.3d at 302). The Amended Complaint alleges that a driver’s license number can be used to file fraudulent unemployment claims, open bank

accounts, apply for credit cards, and take out loans. Am. Compl. ¶ 132–33, 142 [Doc. No. 45]. Further, the Amended Complaint alleges that third parties can use another individual’s driver’s license number to create fake driver’s licenses or to impersonate the victim during a job application process, while receiving medical treatment, and in interactions with law enforcement. Id. at ¶ 134. Because the Amended Complaint alleges that PI exposed in the Data Disclosure can aid various types of fraud, the court can infer that the data is sensitive such that Plaintiffs face a heightened risk of those types of fraud in the future.

MAPFRE asserts that a driver’s license number is less sensitive than a Social Security or credit card number, so the risk of future identity theft from disclosure of a driver’s license number is not imminent and substantial. Mem. ISO Mot. to Dismiss 7 [Doc. No. 49]. In several cases MAPFRE cites to support its argument, however, the complaints at issue either contained no allegations of actual misuse, Hartigan v. Macy’s, Inc., 501 F. Supp. 3d 1, 6 (D. Mass. 2020); see Fus v. CafePress, Inc., 2020 WL 7027653, at *1, (N.D. Ill. Nov. 30, 2020), or did not allege how the information disclosed could be used to commit the types of fraud alleged, Baysal v. Midvale Indem. Co., 78 F.4th 976, 978 (7th Cir. 2023). Similarly, the court in Antman v. Uber Techs., Inc., 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) concluded that the plaintiff’s allegations did not support the conclusion that “harm can come from the misappropriation of a name and a driver’s license.” See also Antman v. Uber Techs., Inc., 2018 WL 2151231, *10–11 (N.D. Cal. May 10, 2018). In contrast, the Amended Complaint here alleges that driver’s license numbers can be used in committing unemployment benefits fraud, debit and credit card fraud, and to open accounts, Am. Compl. ¶¶ 132–33, 142 [Doc. No. 45], and it alleges that some Plaintiffs have suffered these forms of fraud, id. at ¶¶ 53, 75, 83 91, 96. Plaintiffs have thus plausibly alleged that this data constitutes sensitive personal information.

In sum, the Amended Complaint sufficiently alleges injuries in fact. The Amended Complaint includes plausible allegations that some PI stolen in the Data Disclosure has already been misused. It also plausibly alleges a substantial and imminent risk of future fraud stemming from the Data Disclosure such that Plaintiffs' mitigation constitutes a present injury in fact.

3. Traceability

"The 'traceability' or causation element 'requires the plaintiff to show a sufficiently direct causal connection between the challenged action and the identified harm,'" Dantzler, Inc. v. Empresas Berríos Inventory & Operations, Inc., 958 F.3d 38,47 (1st Cir. 2020) (quoting Katz, 672 F.3d at 71), but does not require the plaintiff to show proximate causation, Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 134 n.6 (2014). On a motion to dismiss in the data breach context, plaintiffs must sufficiently allege that the defendant's "actions led to the exposure and actual or potential misuse of the plaintiffs' [PI]." Webb, 72 F.4th at 377.

Plaintiffs sufficiently allege that the instances of actual misuse and efforts to protect themselves against future misuse are traceable to the Data Disclosure. The Amended Complaint alleges that MAPFRE "designed and implemented their own website, which included the instant quote feature that auto-populated Plaintiffs' and Class Members' driver's license numbers in response to the input of basic publicly available consumer information," and that MAPFRE did not implement security measures to prevent unauthorized individuals or bots from obtaining Plaintiffs' information via the Quote Platform. Am. Compl. ¶¶ 12, 160 [Doc. No. 45]. And MAPFRE's notice acknowledged that third parties obtained Plaintiffs' PI "through MAPFRE's Massachusetts online quoting platform." Id. at ¶ 15. Further, as explained above, the Amended Complaint alleges a temporal connection between the instances of fraud and the Data Disclosure; alleges that Plaintiffs are "very careful about sharing [their] PI," id. ¶¶ 41, 47, 55, 63, 68, 77, 85,

98; and alleges that a driver's license number can be used with other information to commit unemployment benefits fraud and open fraudulent lines of credit.

The Amended Complaint also alleges a plausible link between the Data Disclosure and the fraudulent credit and debit card charges that several Plaintiffs incurred. Plaintiffs allege that people in possession of some personal information will purchase driver's license information on the "dark web" to create a complete identity profile and use that profile to commit various forms of identity fraud. *Id.* at ¶¶ 6, 132–35, 137. And one Plaintiff who allegedly incurred fraudulent charges on his debit card, Ma, has received "frequent alerts" that his PI has been discovered on the dark web. *Id.* at ¶ 75. It is reasonable to infer from these allegations that Plaintiffs' PI was harvested in the Data Disclosure and added to existing data sets that enabled those who possessed that data to incur charges on Plaintiffs' existing accounts.

In light of the alleged connections between the PI stolen in the Data Disclosure and identity fraud some Plaintiffs subsequently experienced, a plausible inference may be drawn that the individual or individuals who harvested Plaintiffs' PI in the Data Disclosure used it to commit the alleged fraud or transmitted it to the eventual perpetrator. See *Webb*, 72 F.4th at 374 (explaining "obvious inference" from temporal connection between data breach and instance of fraud, combined with allegations that plaintiff had not otherwise knowingly transmitted PI, was "that the criminal or criminals who filed the false tax return obtained [plaintiff's PI] from the [defendant's] data breach, not from some other source."). The alleged misuse is thus traceable to the Data Disclosure.

MAPFRE argues that the actual misuse alleged in the Amended Complaint is unrelated to the PI disclosed in the Data Disclosure and is thus not traceable to MAPFRE's implementation of the auto-populate feature, citing *Baysal v. Midvale Indemnity Company*, 78 F.4th 976 (7th

Cir. 2023). Memo ISO Mot. to Dismiss 8, 11 [Doc. No. 45]. But in Baysal, plaintiffs did not allege “that knowledge of a driver’s-license number could facilitate” a fraudulent unemployment insurance claim or that “New York State asked for a claimant’s driving information.” 78 F.4th at 978. In contrast, the Amended Complaint here specifically alleges that a driver’s license number can facilitate the types of identity fraud that Plaintiffs allege (which occurred in Massachusetts). Am. Compl. ¶¶ 15, 132.

Further, MAPFRE’s argument that the types of fraud alleged “could not have been committed with the data that was potentially impacted in the Incident” raises factual issues not appropriate for resolution at this stage. See Mem. ISO Mot. to Dismiss 8 [Doc. No. 49]. On a motion to dismiss, the court must take Plaintiffs’ allegations as true. Nisselson v. Lernout, 469 F.3d 143, 150 (1st Cir. 2006). And because the traceability requirement does not require proximate cause, Lexmark Int’l, Inc., 572 U.S. at 134 n.6, “[e]ven a showing that a plaintiff’s injury is indirectly caused by a defendant’s actions satisfies the fairly traceable requirement.” In re MOVEit Customer Data Sec. Breach Litig., 2024 WL 5092276, at *12 (D. Mass. Dec. 12, 2024) (quoting Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012)). Here, Plaintiffs have plausibly alleged that a driver’s license number can aid the forms of financial fraud that they have suffered. Therefore, Plaintiffs have alleged that harm is traceable to exposure of their driver’s license numbers in the Data Disclosure.

The cost of mitigating an imminent and substantial risk of financial fraud is also traceable to MAPFRE’s implementation of the auto-populate feature, which resulted in the Data Disclosure. The Amended Complaint alleges that as a result of the Data Disclosure, third parties continue to possess Plaintiffs’ PI, which can be used to further various forms of identity and financial fraud or can be transmitted to others who can do the same. See Am. Compl. ¶ 129 [Doc.

No. 45]. Therefore, Plaintiffs have sufficiently alleged that their efforts to mitigate the risk of future instances of fraud is traceable to the theft of their PI that was stolen via MAPFRE's Quote Platform.

4. Redressability

a. Damages

Plaintiffs' alleged injuries are redressable with damages. Monetary relief would compensate Plaintiffs for financial harm resulting from fraudulent credit and debit card charges and a delay in obtaining unemployment benefits, as well as for Plaintiffs' time spent responding to those incidents. Further, Ray spent time and effort responding to fraudulent lines of credit opened his name, and all Plaintiffs spent time and effort mitigating the risk of future identity fraud, which resulted in "lost opportunity costs." Am. Compl. ¶¶ 42, 48, 56, 64, 69, 78, 86, 99, 163. That time "is equivalent to a monetary injury" and redressable by damages. Webb, 72 F.4th at 376–77.

b. Declaratory and Injunctive Relief

Plaintiffs lack standing to pursue the prospective relief they seek because such relief will not redress the injury that they allege.

In Webb, the First Circuit held that victims of a data breach failed to allege an injury redressable by the prospective relief they requested. 72 F.4th at 378. First, the court held that an injunction requiring the defendant to implement additional security measures could not protect the plaintiffs from future misuse of their PI by the individuals who had obtained it in the data breach. Id. Additionally, the plaintiffs failed to allege a heightened risk of future data breaches that could be mitigated by an order requiring the defendant to strengthen its data security. Id. Further, the complaint acknowledged that the defendant had made changes that "should have

been in place before” the breach at issue. Id. (emphasis in original). In light of this allegation, the court refused to infer that the prior breach made future exposure more likely. Id. Without sufficient allegations that the plaintiffs faced a heightened risk of a subsequent data breach, the complaint failed to allege an injury that the requested injunction against the defendant would redress. Id.

Plaintiffs here likewise fail to request prospective relief that can redress their alleged injuries. Plaintiffs request “a declaration . . . that Defendants’ existing security measures do not comply with their duties of care to provide adequate security” and an order requiring MAPFRE to implement additional security measures.² Am. Compl. ¶ 247 [Doc. No. 45]. The Amended

² Specifically, Plaintiffs seek measures, including:

- a. Ordering Defendants not to disclose PI, including driver’s license information, to the general public through their website or sales platforms;
- b. Ordering Defendants to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated inquiries by bots, simulated cyber-attacks, penetration tests, and audits on Defendants’ systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors[;]
- c. Ordering Defendants to engage third-party security auditors and internal personnel to run automated security monitoring, including risk analysis on Defendants’ decision making[;]
- d. Ordering Defendants to audit, test, and train their security personnel regarding any new or modified procedures[;]
- e. Ordering Defendants not to make PI available on their Quote Platform[;]
- f. Ordering Defendants not to store PI or make PI accessible in any publicly facing website[;]
- g. Ordering Defendants to purge, delete, and destroy in a reasonably secure manner customer and consumer data not necessary for their provisions of services[;]
- h. Ordering Defendants to conduct regular computer system scanning and security checks; and
- i. Ordering Defendants routinely and continually to conduct internal training and education to inform employees and officers on PI security risks, internal security

Complaint alleges that MAPFRE continues to possess Plaintiffs' PI, so Plaintiffs "are at risk of additional or further harm due to the exposure of their PI and [MAPFRE's] failure to address the security failings that led to such exposure." *Id.* at ¶¶ 243, 245. However, as in *Webb*, the Amended Complaint does not plausibly allege that further exposure is likely to occur. *See Webb*, 72 F.4th at 378. Any suggestion to that effect is undercut by Plaintiffs' acknowledgement that MAPFRE took down its Quote Platform when it became aware of the Data Disclosure. Am. Compl. ¶ 119 [Doc. No. 45]. Further, because third parties have already obtained Plaintiffs' personal information, ordering MAPFRE to better secure that information moving forward would not shield Plaintiffs from identity fraud by those third parties.

In short, the imminent injury Plaintiffs do allege—a heightened risk of future identity theft stemming from the Data Disclosure—is not redressable by an order requiring MAPFRE to improve their data security. And Plaintiffs do not plausibly allege an imminent future injury—a heightened risk of future data breaches—that such an order would redress. Therefore, Plaintiffs lack standing to pursue the declaratory and injunctive relief that they seek.

B. Failure to State a Claim

1. Standard of Review

In evaluating a motion to dismiss for failure to state a claim, the court assumes "the truth of all well-pleaded facts" and draws "all reasonable inferences in the plaintiff's favor." *Nisselson*, 469 F.3d at 150. To survive dismissal, a complaint must contain sufficient factual material to "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550

personnel how to identify and contain a disclosure when it occurs and what to do in response to a data security incident.
Am. Compl. ¶ 247 [Doc. No. 45].

U.S. 544, 570 (2007). “While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations . . . [f]actual allegations must be enough to raise a right to relief above the speculative level” Id. at 545. “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

2. DPPA Violation (Count I)

Plaintiffs allege that MAPFRE violated the DPPA by obtaining motor vehicle records from customers and state agencies and making that information publicly available on the Quote Platform. Am. Compl. ¶¶ 185–86, 191. MAPFRE argues that Plaintiffs’ DPPA claim fails because the Amended Complaint does not allege a “knowing disclosure” of Plaintiffs’ PI “for a purpose not permitted” under the statute. Mem. ISO Mot. to Dismiss 17 [Doc. No. 49]. MAPFRE claims that the Data Disclosure was not a “knowing” disclosure and was instead an instance of theft, and that “unauthorized disclosure to a third party does not constitute a ‘knowing’ disclosure’ under the DPPA.” Id. at 17–18 (emphasis in original).

The DPPA creates a cause of action against an entity that “knowingly obtains, discloses, or uses” an individual’s “personal information” from a motor vehicle record for an impermissible purpose. 18 U.S.C. § 2724. “Personal information” includes “information that identifies an individual,” specifically “including an individual’s . . . driver identification number.” Id. § 2725(1).

Plaintiffs’ Amended Complaint sufficiently alleges a knowing disclosure. Plaintiffs allege that MAPFRE obtained motor vehicle records, including driver’s license numbers, directly from state agencies or through resellers, Am. Compl. ¶ 186 [Doc. No. 45], chose to implement a feature on its Quote Platform that automatically displayed Plaintiffs’ personal information—

including driver’s license numbers—upon entry of other publicly available information, id. at ¶¶ 188–91, and continued operating this feature after DFS published alerts regarding “an ongoing systemic and aggressive campaign” by cybercriminals to obtain information such as unredacted driver’s license numbers from insurance websites that offer instant online automobile insurance quotes, id. at ¶¶ 121, 123–24, 128. In light of alerts from DFS, it is reasonable to infer that MAPFRE knew or should have known that its choice to implement and continue to employ the Quote Platform would expose Plaintiffs’ driver’s license numbers to third parties.

MAPFRE contends that Plaintiffs have failed to allege that MAPFRE disclosed the information for an impermissible purpose. Mem. ISO Mot. 17 [Doc. No. 49]. But the Amended Complaint does allege that MAPFRE implemented the auto-populate feature to “gain a competitive advantage,” i.e. to sell more insurance policies than competitors, Am. Compl. ¶ 10 [Doc. No. 45], and that purpose is not among the permissible purposes set forth at 18 U.S.C. § 2721(b). Because Plaintiffs’ Amended Complaint sufficiently alleges a knowing disclosure for a purpose not permitted under 18 U.S.C. § 2721(b), Plaintiffs have stated a DPPA claim.

3. Negligence (Count II)

To state a negligence claim under Massachusetts law, a plaintiff must allege “that the defendant owed the plaintiff a duty of reasonable care, that the defendant breached this duty, that damage resulted, and that there was a causal relation between the breach of the duty and the damage.” Jupin v. Kask, 447 Mass. 141, 146, 849 N.E.2d 829 (2006). MAPFRE argues that Plaintiffs fail to allege “facts suggesting negligence and assume the unforeseeable criminal conduct of an unknown party is sufficient on its own to maintain a claim.” Mem. ISO Mot. to Dismiss 18–19 [Doc. No. 49]. MAPFRE also asserts that Plaintiffs have not alleged a “measurable loss.” Id. at 19–20.

a. Duty of Care and Breach

“[T]here is a ‘general proposition that there is no duty to protect others from the criminal or wrongful activities of third persons.’” Jupin, 447 Mass. at 148 (quoting Mullins v. Pine Manor Coll., 389 Mass. 47, 50, 449 N.E.2d 331 (1983)). However, “[a]n act or omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person . . . even though such conduct is criminal.” Id. (quoting Restatement (Second) of Torts § 302B (Am. L. Inst. 1965)).

Although the Data Disclosure here involved criminal conduct by third parties, Plaintiffs have alleged negligence by MAPFRE because their alleged harms were a foreseeable result of MAPFRE’s affirmative acts in maintaining the Quote Platform. “In general, anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act.” Restatement (Second) of Torts § 302 cmt. a (Am. L. Inst. 1965). The Amended Complaint alleges that MAPFRE “obtain[ed] motor vehicle records directly from state agencies or through resellers,” “knowingly published” information from such records “to the public on their free online Quote Platform,” and “knowingly linked their . . . public websites to systems and/or networks storing maintaining, and/or obtaining Plaintiffs’ . . . PI.” Am. Compl. ¶¶ 186, 18889 [Doc. No. 45]. These are allegations of affirmative acts that give rise to a duty of care regarding Plaintiffs’ PI. See Portier v. NEO Tech. Sols., 2019 WL 7946103, at *11 (D. Mass. Dec. 31, 2019), report and recommendation adopted, 2020 WL 877035 (D. Mass. Jan. 30, 2020) (“It is reasonable to conclude that [defendant’s] affirmative acts of collecting and storing Plaintiffs’ [PI] gave rise to a duty to exercise due care to safeguard the employees’ [PI].”) (citing Mullins, 389 Mass. at 52–53). And where public notices informed auto insurers that systems like MAPFRE’s Quote

Platform were vulnerable to data theft, the Data Disclosure was a foreseeable result of MAPFRE's continued use of that tool.

b. Damages

MAPFRE argues that Plaintiffs negligence claim fails because they have not “alleged a recoverable loss,” and “[t]he damages claimed by plaintiffs are not cognizable injuries in a negligence claim.” Mem. ISO Mot. 18–19 [Doc. No. 49]. Plaintiffs argue that their allegations of “actual misuse of PI . . . specific quantities of lost time spent mitigating the risk of identity theft, diminution in value of their PI, emotional distress, lost property in the form of compromised PI, a substantial and imminent risk of continued and future misuse of their PI by unauthorized third parties, and injury to their privacy” are sufficient allegations of damages. Opp’n 19–20 [Doc. No. 53].

“A negligence action may not be maintained unless one has suffered injury or damage.” Donovan v. Philip Morris USA, Inc., 455 Mass. 215, 222, 914 N.E.2d 891 (2009) (quoting Cannon v. Sears, Roebuck & Co., 374 Mass. 739, 742, 374 N.E.2d 582 (1978)). Further, “Massachusetts . . . holds that ‘purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage.’” In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009), as amended on reh’g in part (May 5, 2009) (quoting Aldrich v. ADD Inc., 437 Mass. 213, 222, 770 N.E.2d 447 (2002)). The economic loss doctrine generally applies to data breach cases between non-fiduciaries. See, e.g., Cumis Ins. Soc’y, Inc. v. BJ’s Wholesale Club, Inc., 455 Mass. 458, 469–70, 918 N.E.2d 36 (2009) (rejecting argument by card-issuing credit unions that theft of credit card information from retailer amounted to physical harm to tangible property so as to overcome economic loss rule); In re TJX, 564 F.3d at 498–99 (same).

The economic loss doctrine bars Plaintiffs’ negligence claim. Plaintiffs claim for damages based on lost property in the form of compromised PI does not satisfy the property damage requirement. See In re TJX, 564 F.3d at 498–99 (holding loss in value of payment card data did not constitute property damage). Further, assuming the fraudulent credit and debit card activity or the delay in receiving unemployment benefits caused monetary harm, Plaintiffs cannot recover damages for that harm where they have not alleged personal injury or property damage associated with such financial loss. For the same reason, Plaintiffs cannot recover damages for effort and costs associated with mitigating the effects of the Data Disclosure.

Plaintiffs’ allegations of “anxiety, emotional distress,” alarm, and stress associated with the Data Disclosure and mitigation efforts are insufficient to overcome the economic loss doctrine. See Am. Compl. ¶¶ 92, 214 [Doc. No. 45]. Courts have found allegations of “palpable emotional distress” sufficient to satisfy the “personal injury” exception to the economic loss doctrine. See Webb v. Injured Workers Pharmacy, LLC, 2023 WL 5938606, at *3 (D. Mass. Sept. 12, 2023) (citing McCormick v. Lishynsky, 2019 WL 349242 (D.Mass. July 30, 2019) and Maio v. TD Bank, N.A., 2023 WL 2465799, at *4 (D. Mass. Mar. 10, 2023)). “Palpable emotional distress,” however, requires some physical manifestation. See Webb, 2019 WL 34942, *2 (plaintiffs allegedly “suffer from some combination of feelings of rage, anxiety, fear, sleep disruption, stress, and physical pain”); Maio, 2023 WL 2465799, at *4 (allegations of lost sleep, anxiety, and depression); McCormick, 2019 WL 349242, * 5 (allegations of “severe emotional distress, with physical manifestations thereof”). Here, Plaintiffs have not alleged any physical manifestations of their emotional distress. Accordingly, in the absence of allegations of physical injury or property damage, their negligence claim may not proceed.

4. Massachusetts General Laws, Chapter 93A (Count III)

The Amended Complaint alleges that MAPFRE violated M.G.L. c. 93A §2 regarding Ma and Devereaux, the Massachusetts Plaintiffs. Am. Compl. ¶ 219 [Doc. No. 45]. M.G.L. c. 93A § 2 prohibits “[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce” The Amended Complaint alleges that MAPFRE’s knowing implementation of a website feature that disclosed Plaintiffs’ driver’s license number upon entry of minimal personal information without deploying adequate security measures is an unfair business practice that caused the Massachusetts Plaintiffs’ various alleged injuries. See Am. Compl. ¶¶ 220–27 [Doc. No. 45].

MAPFRE argues that the Amended Complaint fails to allege that MAPFRE benefitted from sufficiently unfair business practices at Plaintiffs’ expense. Mem. ISO Mot. to Dismiss 21 [Doc. No. 49]. That is, MAPFRE’s implementation of the Quote Platform is not conduct that rises to the level of unfairness required to state a claim under the statute, and this conduct did not cause Plaintiffs’ alleged injuries. Id.

To state a claim under the consumer protection statute, [Mass. Gen. Laws ch. 93A, § 9], a plaintiff must allege facts sufficient to establish four elements: first, that the defendant has committed an unfair or deceptive act or practice; second, that the unfair or deceptive act or practice occurred ‘in the conduct of any trade or commerce;’ third, that the plaintiff suffered an injury; and fourth, that the defendant's unfair or deceptive conduct was a cause of the injury.

Rafferty v. Merck & Co., Inc., 479 Mass. 141, 161, 92 N.E.3d 1205 (2018).

In determining whether an act is “unfair” within the meaning of the statute, courts consider “(1) whether the practice . . . is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers” Mass. Eye & Ear Infirmary v. QLT Phototherapeutics, Inc., 412 F.3d 215, 243 (1st Cir. 2005)

(quoting PMP Assocs., Inc. v. Globe Newspaper Co., 366 Mass. 593, 596, 321 N.E.2d 915 (1975)). “To rise to the level of an ‘unfair’ act or practice, the defendant’s conduct must generally be of an egregious, non-negligent nature.” Walsh v. TelTech Sys., Inc., 821 F.3d 155, 160 (1st Cir. 2016). An injury for Chapter 93A purposes must be separate from the unfair or deceptive conduct. Id. at 161 (“[T]he violation of an independent statute . . . does not itself ‘satisf[y] the injury requirement of c. 93A, § 9.’”) (second alteration in original) (citing Tyler v. Michaels Stores, Inc., 464 Mass. 492, 502, 984 N.E.2d 737 (2013)).

Plaintiffs’ allegations are sufficient for their Chapter 93A claim to proceed. First, Plaintiffs have alleged conduct—MAPFRE’s use of a website feature that it knew could lead to dissemination of Plaintiffs’ personal information without accompanying security measures—that at least arguably violates Plaintiffs’ DPPA rights and right to privacy. Second, the Amended Complaint alleges that MAPFRE implemented this feature for the purpose of increasing insurance sales, i.e. in the conduct of commerce. UBS Fin. Servs., Inc. v. Aliberti, 483 Mass. 396, 411, 113 N.E.3d 277 (2019) (explaining “‘trade or commerce’ requirement is met when the defendant was operating in ‘a business context’ at the time of its allegedly unfair . . . activity,” and “business context” inquiry depends in part on whether conduct “was motivated by business or personal reasons”) (internal citations omitted). Third, as explained above, the Amended Complaint alleges actual misuse of some PI and risk mitigation costs, which are injuries distinct from the mere invasion of Plaintiffs’ protected rights. Cf. Tyler, 464 Mass at 50304 & n.17 (explaining that acquiring personal information in violation of privacy statute causes an injury distinct from the statutory violation if that information is subsequently used for business purposes). Fourth, the Complaint sufficiently alleges that Plaintiffs’ injuries are a result of MAPFRE’s implementation of the auto-populate feature.

5. Invasion of Privacy (Count IV)

The Amended Complaint alleges that MAPFRE's obtaining Plaintiffs' driver's license numbers and its exposure of that information through the Quote Platform were "unreasonable, substantial, and serious invasion[s] of Plaintiffs' privacy." Am. Compl. ¶ 236–37 [Doc. No. 45]. MAPFRE argues that Plaintiffs' allegations are insufficient because the Amended Complaint fails to allege any intentional conduct by MAPFRE that could have been the legal cause of the exposure of Plaintiffs' PI, which was disclosed due to intentional conduct by an unauthorized third party. Mem. ISO Mot. to Dismiss 21–22 [Doc. No. 49]. MAPFRE also argues that Plaintiffs fail to allege actual damages stemming from the alleged invasion of privacy. Id.

In Massachusetts, individuals are protected against invasions of privacy by statute. Massachusetts General Laws ch. 214, § 1B, recognizes "a right against unreasonable, substantial or serious interference with his privacy." M.G.L c. 214, § 1B. To maintain a claim under § 1B, plaintiffs must allege "a 'gathering and dissemination of privation information' by the defendant." In re Shields Health Care Grp., Inc. Data Breach Litig., 721 F. Supp. 3d 152, 164 (D. Mass. 2024) (citing Nelson v. Salem State Coll., 446 Mass. 525, 536, 845 N.E.2d 338 (2006)) (emphasis added).

Plaintiffs fail to state an invasion-of-privacy claim here. Although the Amended Complaint alleged MAPFRE's actions enabled third parties to obtain Plaintiffs' PI, it does not allege that MAPFRE disseminated their PI. The Amended Complaint alleges that MAPFRE obtained Plaintiffs' PI and that MAPFRE implemented the auto-populate feature knowing such a feature could expose that information to unauthorized third parties. See, e.g., Am. Compl. ¶ 128 [Doc. No. 45]. However, the Amended Complaint acknowledges that a third party has to take some additional action to obtain driver's license information from the Quote Platform. Id.

(“Defendants also knew that [the Quote Platform] . . . allowed fraudsters to plug in readily, publicly available basic PI of other persons, and that the website would auto-populate driver’s license information once that basic information was entered.”) Although Plaintiffs allege that third parties could exploit the Quote Platform to obtain their PI using minimal, publicly available information, that allegation demonstrates that MAPFRE itself did not disseminate Plaintiffs’ PI. Because Plaintiffs fail to allege dissemination by MAPFRE, their invasion of privacy claim fails. See In re Shields Health Care Grp., 721 F. Supp. 3d at 164 (D. Mass. 2024); but see Shedd v. Sturdy Mem’l Hosp., Inc., 2022 WL 1102524, at *11 (Mass. Super. Apr. 5, 2022) (“Plaintiffs allege that unauthorized persons gained access to their personal and highly confidential information due to Sturdy Memorial’s inadequate, negligent and/or intentionally insufficient security measures They have stated a claim for invasion of privacy.”).

6. Declaratory Relief (Count V)

Above, the court has determined that Plaintiffs do not have standing to pursue declaratory relief. Therefore, the court does not need to address MAPFRE’s argument that Plaintiffs fail to state a claim for a declaratory judgment.

III. Conclusion

For the foregoing reasons, Defendants’ Motion to Dismiss [Doc. No. 48] is DENIED as to Counts I (violation of the Driver’s Privacy Protection Act) and III (violation Chapter 93A) and GRANTED as to Counts II (Negligence), IV (Invasion of Privacy), and V (Declaratory Relief).

IT IS SO ORDERED.

March 31, 2025

/s/Indira Talwani
United States District Judge